Deploy the ExtraHop Explore Appliance with VMware

Published: 2021-10-13

In this guide, you will learn how to deploy the ExtraHop Explore virtual appliance with the vSphere client running on a Windows machine and to join multiple Explore appliances to create an Explore cluster. You should be familiar with administrating VMware ESX and ESXi environments before proceeding.

The Explore virtual appliance is distributed as an OVA package that includes a preconfigured virtual machine (VM) with a 64-bit, Linux-based OS that is optimized to work with VMware ESX and ESXi version 5.5 and later.

Important: If you want to deploy more than one ExtraHop virtual appliance, create the new instance with the original deployment package or clone an existing instance that has never been started.

System requirements

Your environment must meet the following requirements to deploy a virtual Explore appliance:

Important: ExtraHop tests virtual Explore clusters on local storage for optimal performance. ExtraHop strongly recommends deploying virtual Explore clusters on continuously available, low latency storage, such as a local disk, direct-attached storage (DAS), network-attached storage (NAS), or storage area network (SAN).

- An existing installation of VMware ESX or ESXi server version 5.5 or later capable of hosting the Explore virtual appliance. The Explore virtual appliance is available in the following configurations:

EXA Master Node	EXA-XS	EXA-S	EXA-M	EXA-L
4 CPUs	4 CPUs	8 CPUs	16 CPUs	32 CPUs
8 GB RAM	8 GB RAM	16 GB RAM	32 GB RAM	64 GB RAM
4 GB boot disk	4 GB boot disk	4 GB boot disk	4 GB boot disk	4 GB boot disk
12 GB	250 GB or smaller datastore disk	500 GB or smaller datastore disk	1 TB or smaller datastore disk	2 TB or smaller datastore disk

  The hypervisor CPU should provide Supplemental Streaming SIMD Extensions 3 (SSSE3) support.

  Note: The Explore master node is preconfigured with a 12 GB datastore disk. You must manually configure a second virtual disk to the other EXA configurations to store record data.

  Consult with your ExtraHop sales representative or Technical Support to determine the datastore disk size that is best for your needs.
- A vSphere client
- An Explore virtual appliance license key.
- The following TCP ports must be open:
  - TCP ports 80 and 443: Enables you to administer the Explore appliance. Requests sent to port 80 are automatically redirected to HTTPS port 443.
  - TCP port 9443: Enables Explore nodes to communicate with other Explore nodes in the same cluster.

Deploy the Explore virtual appliance

Before you begin
If you have not already done so, download the ExtraHop Explore virtual appliance OVA file for VMware from the ExtraHop Customer Portal.

Note: If you must migrate the VM to a different host after deployment, shut down the virtual appliance first and then migrate with a tool such as VMware VMotion. Live migration is not supported.

1. Start the VMware vSphere client and connect to your ESX server.
2. Go to the File menu and select **Deploy OVF Template**.
3. The steps to deploy the OVF template are described in detail below. For most deployments, the default settings are sufficient.
   a) Source: Browse to the location of the downloaded OVA file and then click **Next**.
   b) OVF Template Details: Review the details and then click **Next**.
   c) Name and Location: Configure the VM name and location. Give the VM a unique and specific name for the ESX Inventory and then click **Next**.
   d) Disk Format: Select **Thick Provision Lazy Zeroed** and then click **Next**.
   e) Network Mapping: Map the OVF-configured network interface labels with the correct ESX-configured interface labels and then click **Next**.
   f) Ready to Complete: Verify the configuration, do not select the Power on after deployment checkbox, and then click **Finish** to complete the deployment.

   When the deployment is complete, you can see the unique name you assigned to the Explore appliance VM instance in the inventory tree for the ESX server to which it was deployed.
4. Click the new Explore appliance VM instance in the directory tree.
5. From the Actions drop-down list, select **Edit Settings...** to configure the disk where the Explore appliance data is stored.
6. From the New device drop-down list, select **New Hard Disk**, confirm that **Thick Provision Lazy Zeroed** is selected for Disk Provisioning and then click **Add**.
7. In the New Hard disk field, type the size of your virtual storage disk and then click **OK**.
8. From the Actions drop-down list, select **Power On**.
9. From the Actions drop-down list, select **Open Console**.
10. Log in with the `shell` user account. Type `default` for the password.
11. Run the `show ipaddr` command to display the IP address of the Explore virtual appliance.
12. Exit the console window.

Configure a static IP address through the CLI

The ExtraHop system is delivered with DHCP enabled. If your network does not support DHCP, no IP address is acquired, and you must configure a static address manually.

Important: For deployments that include a Discover appliance that is connected to a Command appliance, we strongly recommend configuring a unique hostname. If the IP address on the sensor is changed, the Command appliance can re-establish connection easily to the sensor by hostname.

1. Access the CLI through an SSH connection, by connecting a USB keyboard and SVGA monitor to the appliance, or through an RS-232 serial cable and a terminal emulator program. The terminal emulator must be set to 115200 bps with 8 data bits, no parity, 1 stop bit (8N1), and hardware flow control should be disabled.
2. At the login prompt, type `shell` and then press ENTER.

3. At the password prompt, type `default`, and then press ENTER.
4. To configure the static IP address, run the following commands:
   a) Enable privileged commands:

   ```
   enable
   ```

   b) At the password prompt, type `default`, and then press ENTER.
   c) Enter configuration mode:

   ```
   configure
   ```

   d) Enter the interface configuration mode:

   ```
   interface
   ```

   e) Run the `ip` command and specify the IP address and DNS settings in the following format: `ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`
   For example:

   ```
   ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
   ```

   f) Leave the interface configuration section:

   ```
   exit
   ```

   g) Save the running config file:

   ```
   running_config save
   ```

   h) Type y and then press ENTER.

Configure the Explore appliance

After you obtain the IP address for the Explore appliance, log in to the appliance through `https://<explore_ip_address>/admin` and complete the following recommended procedures.

Note: The default login username is `setup` and the password is `default`.

- Register your ExtraHop system
- Connect the Discover and Command appliances to Explore appliances
- Send record data to the Explore appliance
- Review the Explore Post-deployment Checklist and configure additional Explore appliance settings.

Create an Explore cluster

For the best performance, data redundancy, and stability, you must configure at least three Explore appliances in an Explore cluster.

Important: If you are creating an Explore cluster with six or more nodes, you must configure the cluster with master nodes. For master node instructions, see Deploying master nodes.

In the following example, the Explore appliances have the following IP addresses:

- Node 1: 10.20.227.177
- Node 2: 10.20.227.178
- Node 3: 10.20.227.179

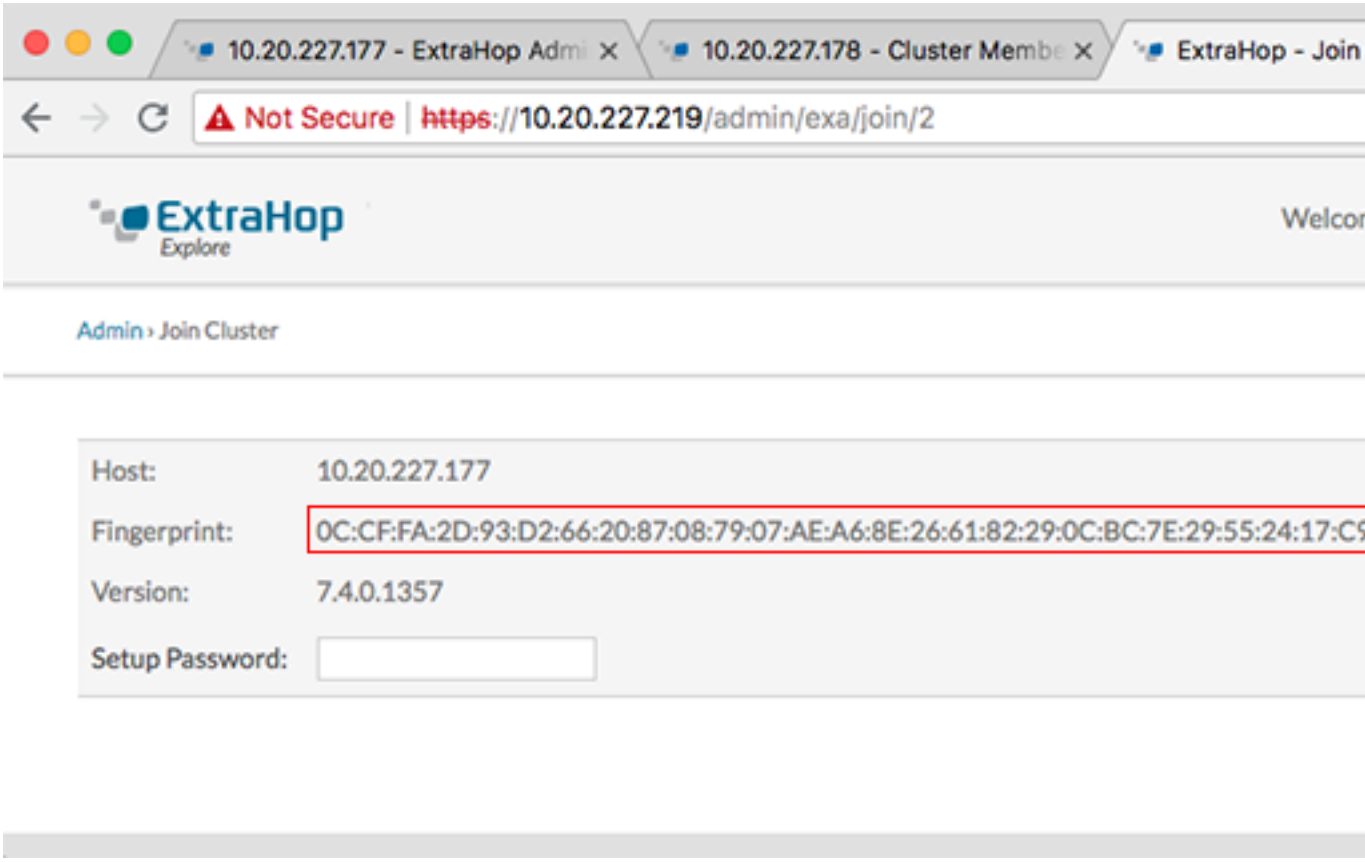
You will join nodes 2 and 3 to node 1 to create the Explore cluster. All three nodes are data nodes. You cannot join a data node to a master node or join a master node to a master node to create a cluster.

Important: Each node that you join must have the same configuration (physical or virtual) and the same ExtraHop firmware version. EXA 5100 and EXA 5200 physical appliances can be in the same cluster.

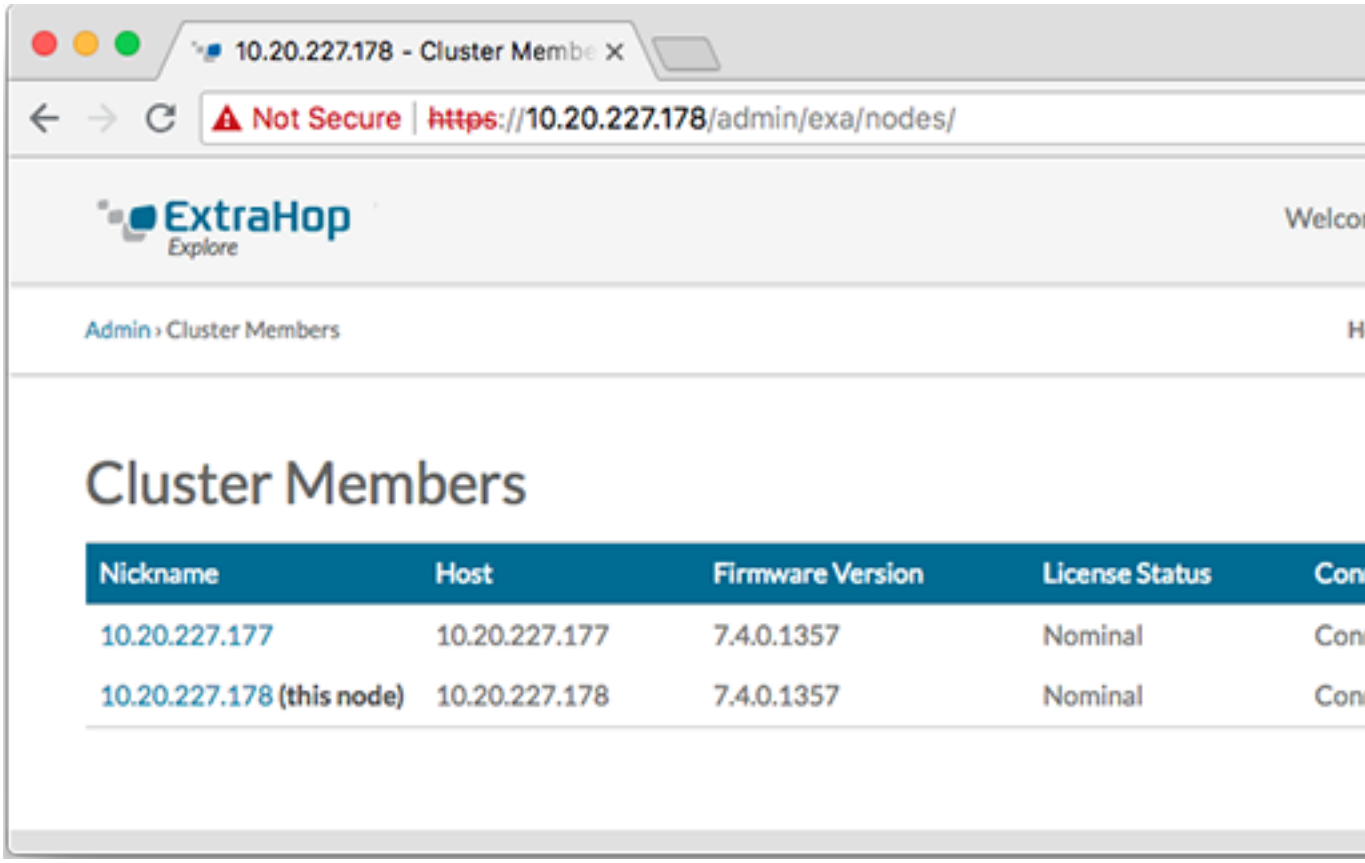
Before you begin
You must have already installed or provisioned the Explore appliances in your environment before proceeding.

1. Log in to the Administration settings on all three Explore appliances with the setup user account in three separate browser windows or tabs.
2. Select the browser window of node 1.
3. In the Status and Diagnostics section, click **Fingerprint** and note the fingerprint value. You will later confirm that the fingerprint for node 1 matches when you join the remaining two nodes.
4. Select the browser window of node 2.
5. In the Explore Cluster Settings section, click **Join Cluster**.
6. In the Host field, type the hostname or IP address of data node 1 and then click **Continue**.

   Note: For cloud-based deployments, be sure to type the IP address listed in the Interfaces table on the Connectivity page.
7. Confirm that the fingerprint on this page matches the fingerprint you noted in step 3.

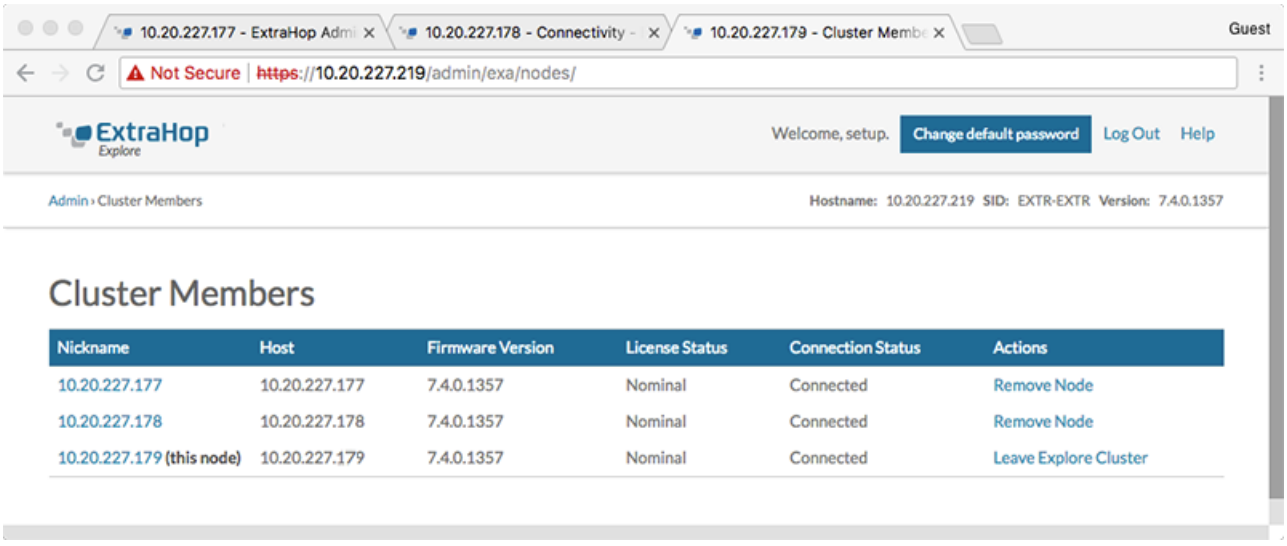


8. In the Setup Password field, type the password for the node 1 `setup` user account and then click **Join**. When the join is complete, the Explore Cluster Settings section has two new entries: **Cluster Members** and **Cluster Data Management**.
9. Click Cluster Members. You should see node 1 and node 2 in the list.



10. In the Status and Diagnostics section, click **Explore Cluster Status**. Wait for the Status field to change to `Green` before adding the next node.
11. Repeat steps 5 - 10 to join each additional node to the new cluster.

    Note: To avoid creating multiple clusters, always join a new node to an existing cluster and not to another single appliance.
12. When you have added all of your Explore appliances to the cluster, click **Cluster Members** in the Explore Cluster Settings section. You should see all of the joined nodes in the list, similar to the following figure.



13. In the Explore Cluster Settings section, click **Cluster Data Management** and make sure that **Replication Level** is set to **1** and **Shard Reallocation** is **ON**.

Next steps
Connect the Discover and Command appliances to Explore appliances

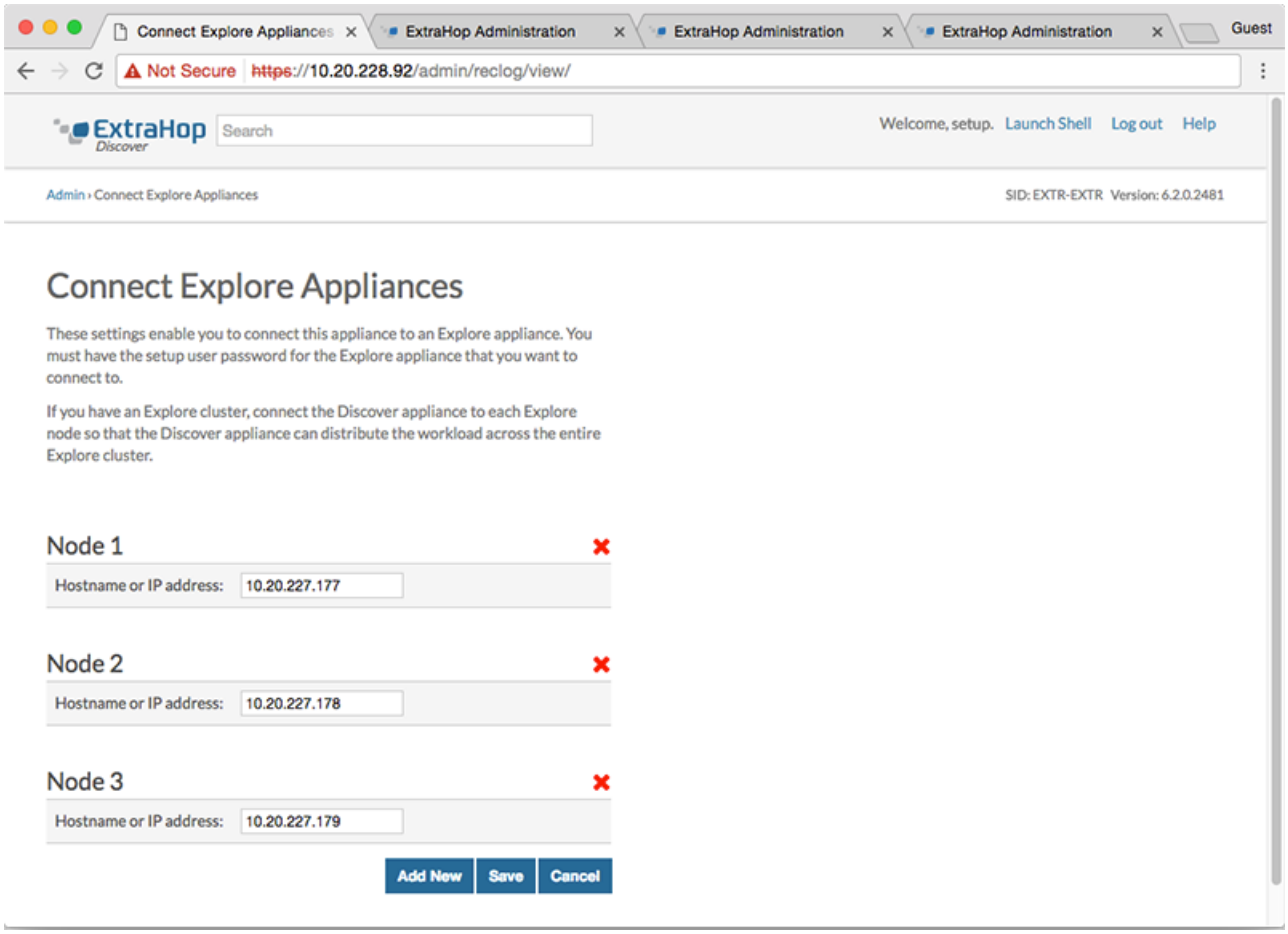
Connect the Explore appliance to Discover and Command appliances

After you deploy the Explore appliance, you must establish a connection from all ExtraHop Discover and Command appliances to the Explore appliance before you can query records.

Important: If you have an Explore cluster of three or more Explore nodes, connect the Discover appliance to each Explore node so that the Discover appliance can distribute the workload across the entire Explore cluster.

Note: If you manage all of your Discover appliances from a Command appliance, you only need to perform this procedure from the Command appliance.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the ExtraHop Explore Settings section, click **Connect Explore Appliances**.
3. Click **Add New**.
4. In the Explore node field, type the hostname or IP address of any Explore appliance in the Explore cluster.
5. For each additional Explore appliance in the cluster, click **Add New** and enter the individual hostname or IP address in the corresponding Explore node field.



6. Click **Save**.

7. Confirm that the fingerprint on this page matches the fingerprint of node 1 of the Explore cluster.
8. In the Explore Setup Password field, type the password for the Explore node 1 `setup` user account and then click **Connect**.
9. When the Explore Cluster settings are saved, click **Done**.

Send record data to the Explore appliance

After your Explore appliance is connected to all of your Discover and Command appliances, you must configure the type of records you want to store.

See Records for more information about configuration settings, how to generate and store records, and how to create record queries.